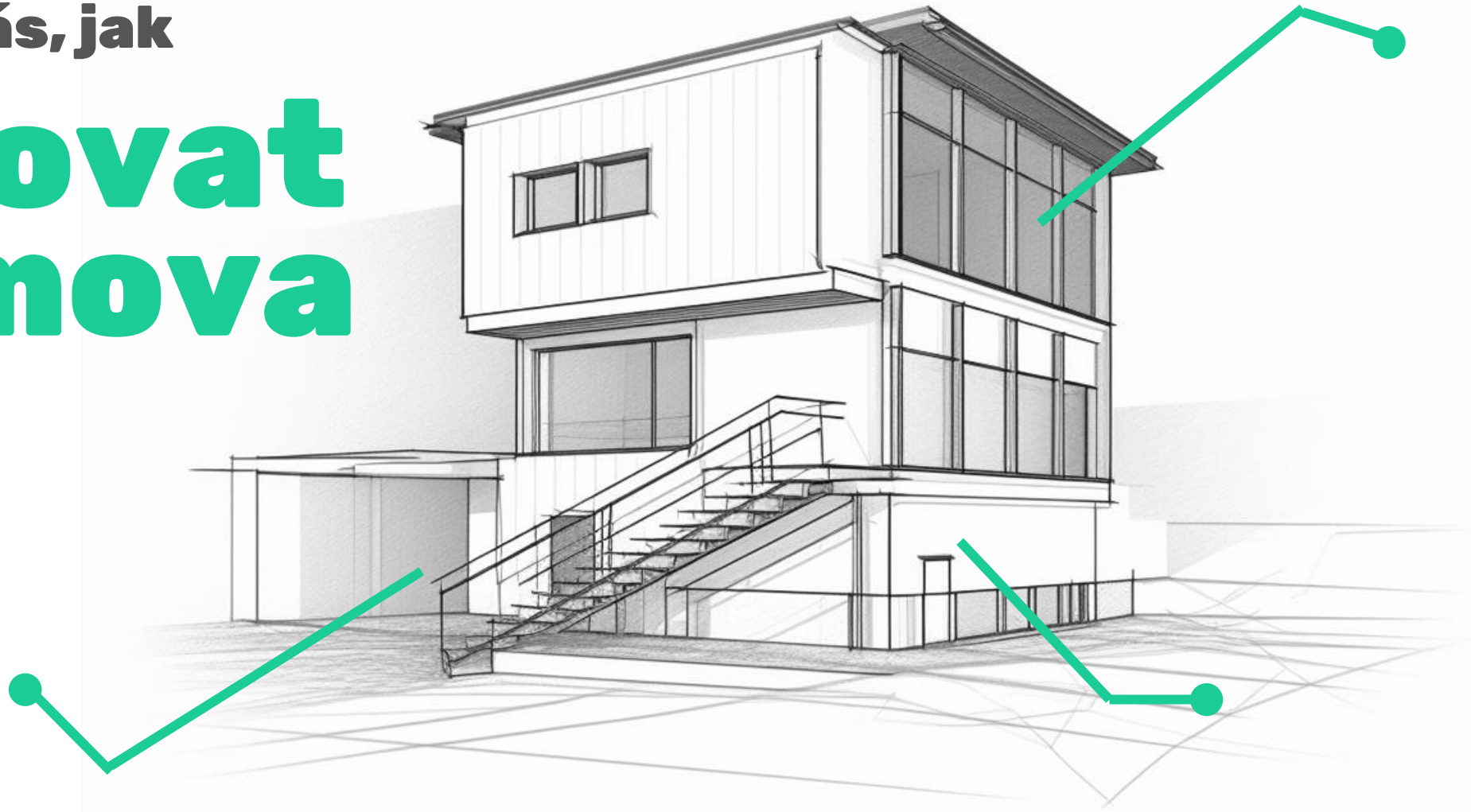
CYBEREADY

## Návod pro vás, jak

# pracovat z domova



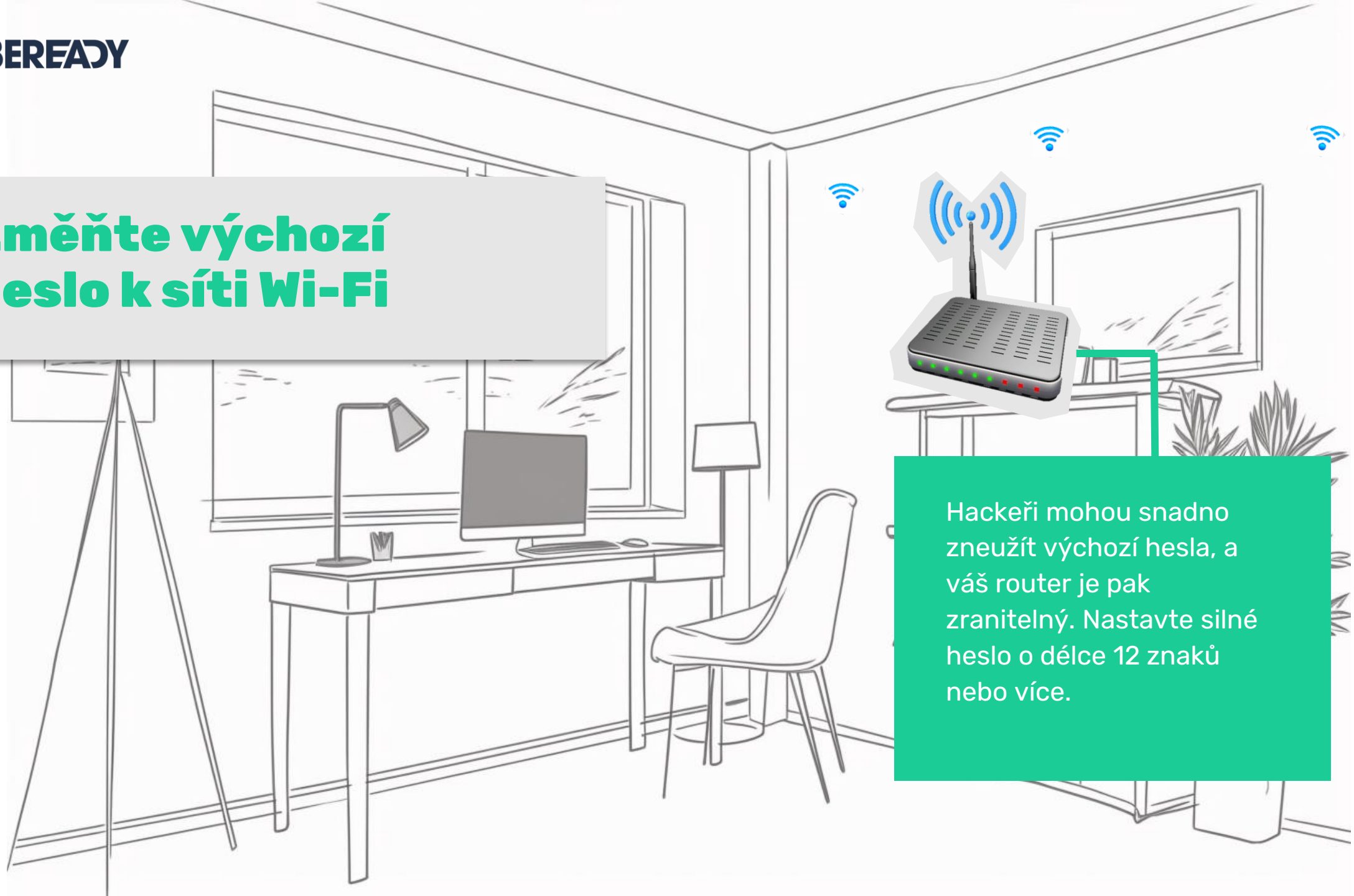
CYBEREADY

**Práce na dálku vyžaduje zcela jiný přístup k zabezpečení.**
**Ukážeme vám, jak zachováte bezpečnost v následujících oblastech:**

1. Heslo pro Wi-Fi
2. Zařízení
3. Pracovní prostor
4. Cestování
5. Technická podpora
6. Bezpečnostní zálohování

CYBEREADY

# Změňte výchozí heslo k síti Wi-Fi



Hackeři mohou snadno zneužít výchozí hesla, a váš router je pak zranitelný. Nastavte silné heslo o délce 12 znaků nebo více.

# Pracujte pouze na zařízeních poskytnutých firmou

Pracovní dokumenty nemají co dělat na osobních zařízeních! (Obvykle nejsou vybavena účinnými bezpečnostními funkcemi.) Pokud je přístup ke kalendáři, e-mailu a aplikacím pro rychlé zasílání zpráv na vašem osobním smartphonu nezbytný, vyvarujte se sdílení citlivých údajů.

# Udržujte bezpečnost firemní techniky

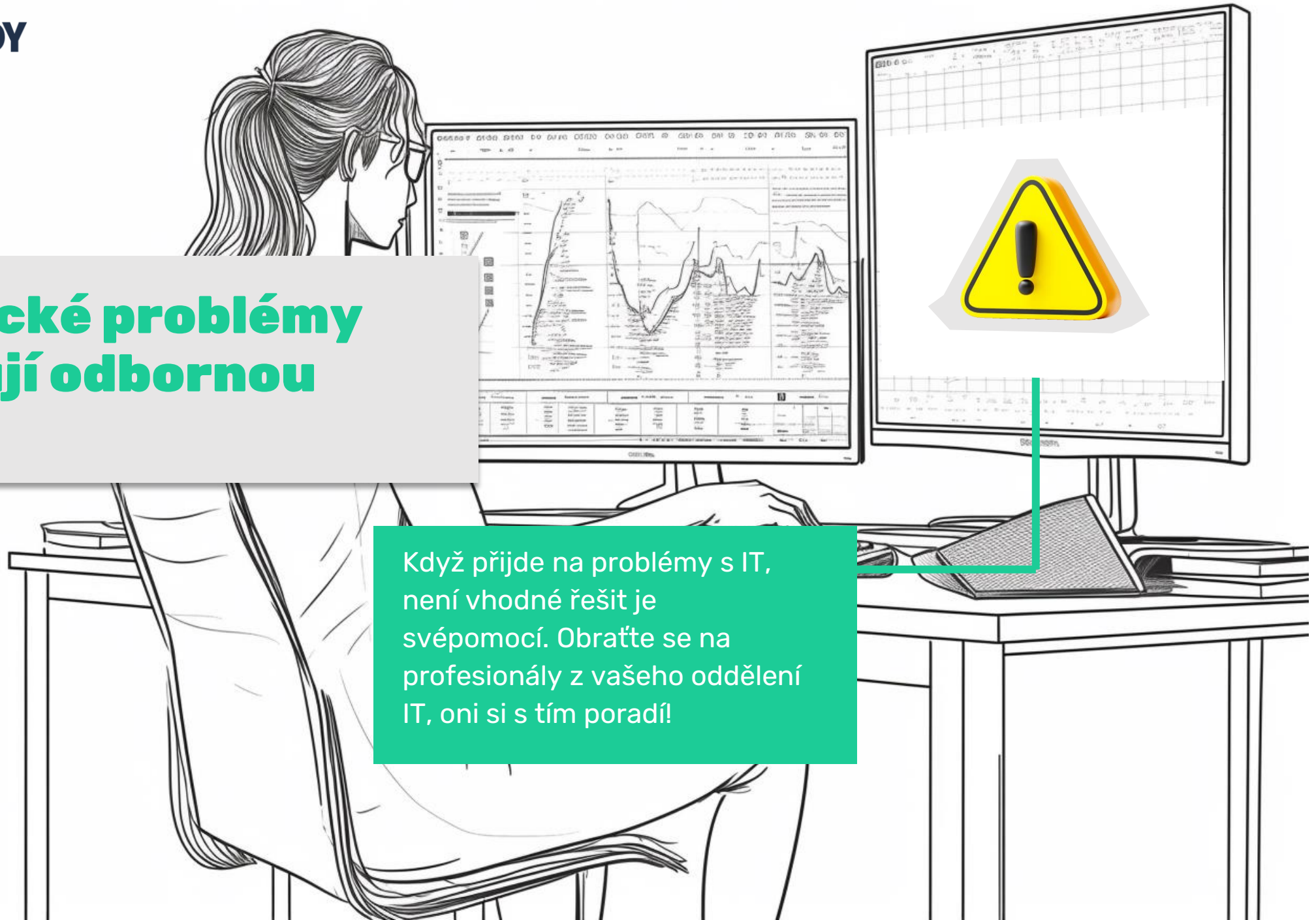
Zabraňte neoprávněnému přístupu k citlivým materiálům tím, že vytvoříte vyhrazený pracovní prostor pouze pro své použití (bez přátel nebo rodiny).

# Chraňte svá zařízení, když cestujete

Opouštíte domov na 48 nebo více hodin? Uložte bezpečně pracovní zařízení, anebo zajistěte, aby byla chráněna, zatímco jste na cestách.

CYBEREADY

# Technické problémy vyžadují odbornou pomoc



Když přijde na problémy s IT, není vhodné řešit je svépomocí. Obraťte se na profesionály z vašeho oddělení IT, oni si s tím poradí!

CYBEREADY

# Máte pochybnosti o zabezpečení? Obraťte se na nás.

Uvolněte se a nebuďte pod tlakem! Bezpečnostní tým je tu pro vás. Máme potřebné znalosti pro ochranu vašich zařízení a dat bez ohledu na konkrétní scénář.